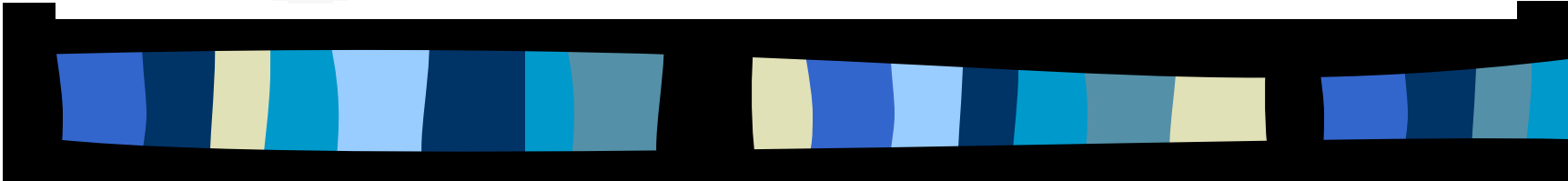




FEDERAL TRADE COMMISSION

WORKING FOR CONSUMER PROTECTION
AND A COMPETITIVE MARKETPLACE



The Gramm-Leach-Bliley Act Final Rule on Safeguards for Customer Financial Information



About this presentation . . .

- The views expressed in this presentation are those of the speaker and not necessarily those of the Commission or any individual Commissioner.
- For more detailed information, visit the FTC's homepage at www.ftc.gov .



FTC Safeguards Rule

- Implements the security provisions of the Gramm-Leach-Bliley Act of 1999.
- Took effect May 23, 2003, with an extra year to conform third-party service provider contracts entered into prior to June 24, 2002.
- Has flexible standard, but imposes certain basic requirements. See 67 Fed. Reg. 36484.



Standard for Safeguards

- Each financial institution must develop, implement and maintain a comprehensive information security program that is written in readily accessible part(s);
- The program must contain administrative, technical and physical safeguards that are appropriate to:
 - the size and complexity of the financial institution;
 - the nature and scope of its activities; and
 - the sensitivity its customer information.
- Although the standard is flexible, the Rule sets forth certain required elements for information security programs.



Required Elements – Each financial institution must:

- Designate one or more employees to coordinate its program;
- Assess risks to the security of customer information;
- Design and implement safeguards to address these risks, and test and monitor their effectiveness over time;
- Oversee service providers; and
- Adjust the program to address developments.



Areas of Operation--

To assess risks and design safeguards, a financial institution must consider all relevant areas of its operation, including:

- (1) Employee training and management;
- (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal;
- (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.



Oversight of Service Providers*

- (1) Take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and
- (2) Require service providers by contract to implement and maintain such safeguards.

* Service providers are companies that handle or have access to customer information in the course of providing services directly to a financial institution.



Who is covered by the Rule?

- Applies to financial institutions under the FTC's jurisdiction;
- Includes financial institutions that receive customer information from another financial institution.





What is a financial institution?

- Any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956. An institution that is significantly engaged in financial activities is a financial institution.



Regulations define “financial activities”

- Lending, exchanging, transferring, investing for others, or safeguarding money or securities. [4(k)(4)(A)]
- An activity that the Federal Reserve Board has determined to be closely related to banking. [4(k)(4)(F); 12 C.F.R. 225.28]
 - Extending credit and servicing loans
 - Collection agency services
- An activity that a bank holding company may engage in outside the U.S. [4(k)(4)(G); 12 C.F.R. 211.5].



Examples of financial activities

- Mortgage broker
- Check casher
- Pay-day lender
- Credit counseling service
- Retailer that issues its own credit card
- Auto dealers that lease and/or finance



What information is covered?

- “Customer information,” which means:
 - (1) Nonpublic personal information concerning its own customers; and
 - (2) Nonpublic personal information that it receives from a financial institution about the customers of another financial institution;
- NOTE: Customer information includes information handled by affiliates.



Affiliates

- If a financial institution shares customer information with its affiliates, it must ensure that the affiliates have adequate safeguards in place.
- Affiliate means any company that controls, is controlled by, or is under common control with another company. See Privacy Rule, section 313.3(a).



Relationship to FTC's Privacy Rule

- Both Rules implement section 501 of the GLBA.
- The Safeguards Rule uses Privacy Rule definitions, but defines new terms “customer information” and “service provider.”
- The Privacy Rule focuses on Privacy Notices, Opt Out rights and limits on use and disclosure; the Safeguards Rule focuses on security.



FEDERAL TRADE COMMISSION

WORKING FOR CONSUMER PROTECTION
AND A COMPETITIVE MARKETPLACE

For more information, see
<http://www.ftc.gov/privacy/index.html>